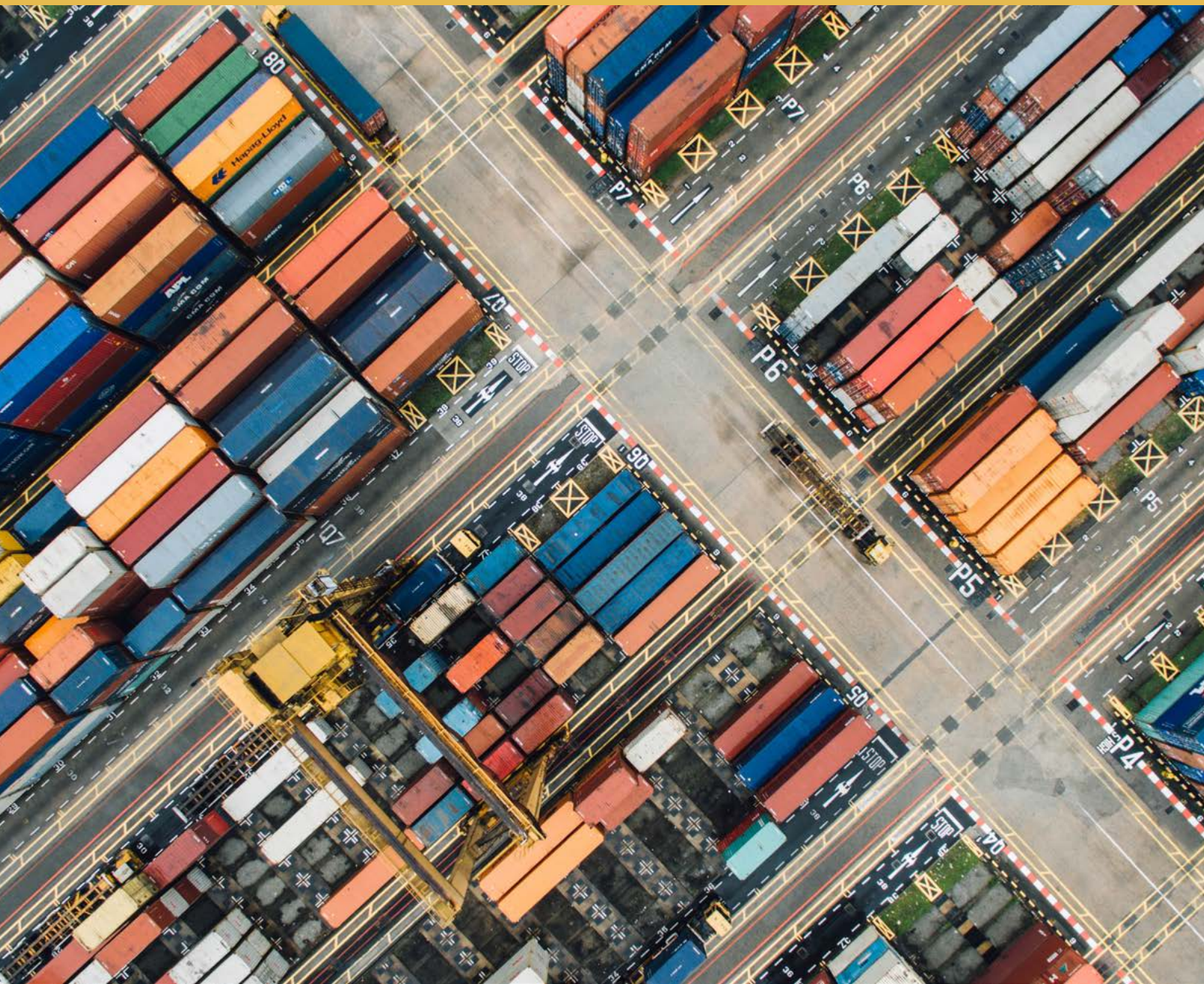


Enterprise Risk

Summer 2021 / www.enterpriseriskmag.com

The official magazine of the Institute of Risk Management

Chain reactions: The pandemic is wreaking havoc in global supply chains, yet businesses often fail to have a basic overview of their operations



Relationship trouble: what interconnected supply chains really mean / **Quantum effects:** ESG in radical uncertainty / **Buyer beware:** navigating software purchases / **Digital innovation:** IRM explores advanced technologies

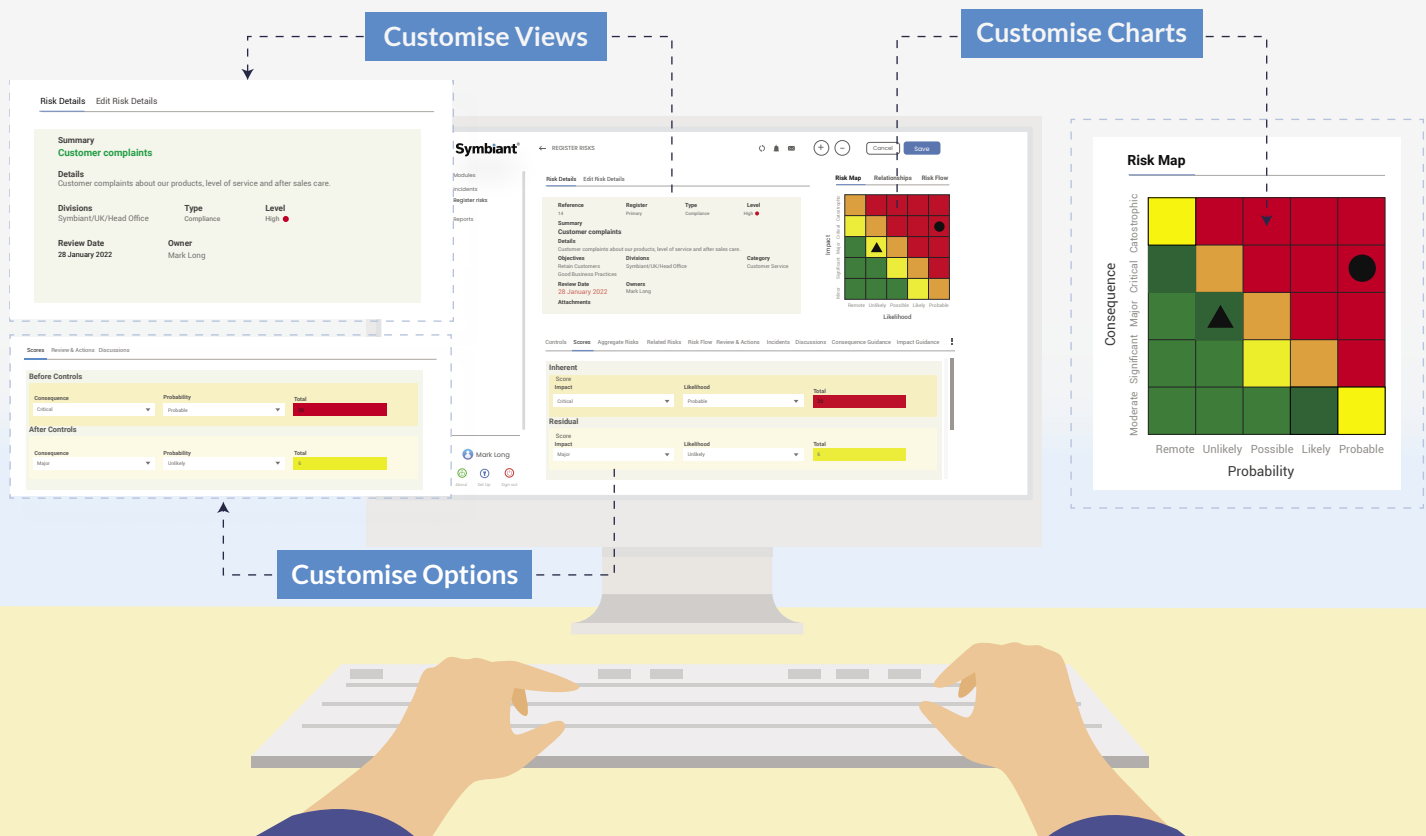
Symbiant®

The Most Powerful, Flexible and Affordable Risk, Audit and Compliance Management System Ever Built

Symbiant is a ready-made off the shelf solution that can be customised to meet your **EXACT** requirements.

We include a **FREE** customisation service so you can have your perfect solution at no extra cost.

[Visit our website and watch the overview video](#)



For more information or a free trial, please visit our web site
www.symbiant.uk

Editor
Arthur Piper

Produced by
Smith de Wint
Cobden Place, 5 Cobden Chambers
Pelham Street, Nottingham, NG1 2ED
Tel: +44 (0)115 958 2024
risk@sdw.co.uk
www.sdw.co.uk

**Sponsorship and
Advertising Sales Manager**
Redactive Media
IRMsales@redactive.co.uk
Tel: +44(0)20 7324 2753

Enterprise Risk is the official publication of
the Institute of Risk Management (IRM).

ISSN 2397-8848

About the IRM

The IRM is the leading professional
body for Enterprise Risk Management
(ERM). We drive excellence in managing
risk to ensure organisations are ready for
the opportunities and threats of the future.

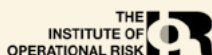
We do this by providing internationally
recognised qualifications and training,
publishing research and guidance, and
setting professional standards.

For over 30 years our qualifications have
been the global choice of qualification for
risk professionals and their employers.

We are a not-for-profit body,
with members working in all industries,
in all risk disciplines and in all sectors
around the world.

Institute of Risk Management
2nd Floor, Sackville House, 143-149
Fenchurch Street, London, EC3M 6BN
Tel: +44 (0)20 7709 9808
Fax: +44 (0)20 7709 0716
enquiries@theirm.org
www.theirm.org

Copyright © 2021 Institute of Risk
Management. All rights reserved.
Reproduction without written permission
is strictly forbidden. The views of outside
contributors are not necessarily the views
of IRM, its editor or its staff.



Enterprise risk – a new look

We have been working behind the scenes for the last few months to refresh the look and feel of Enterprise risk. You have the results in your hand now – either online, mobile or in print. And we hope you like the results.

Publishing, like all industries today, is beset with rapid change. As risk managers, you know better than most what such change brings – risk and opportunity. Even in the four years since I have been editing this publication, digital innovations have greatly altered the way we all consume media. The challenge is to take advantage of that diversity while maintaining a core, quality product – the magazine.

“ The design is smarter and more streamlined – more connected to the wider world of information in which it operates

That is why many of the changes we have made are subtle design tweaks that should make pages and images more suited to being consumed on digital platforms. We can connect to video, audio and other media through the magazine more easily now, enabling us to curate a wider range of content to inform and stimulate. The design is smarter and more streamlined – more connected to the wider world of information in which it operates.

One of the fun aspects of editing a publication is that this process continues well after the first issue comes into existence. As we work with the new format, we will get a better feel for what it can achieve and, hopefully, use our creativity to experiment with more interesting ways of conveying the stories our contributors tell.

That segues a bit tangentially into the main theme of our content for this issue – the interconnected nature of the world in which we live. From the supply chain special issue (pages 10-21) to Peadar Duffy's notion of quantum risk (pages 22-27), it seems clear to me that the disruption of the last year or so has pushed this notion much higher up the boardroom agenda. It is not that businesses did not know about such interdependencies; it is that most have experienced them much more forcefully and immediately because of the pandemic.

Navigating that landscape requires organisations to become more responsive and engaged with their suppliers and with the communities in which they operate. Those who are most alive to the reality outside of their organisations will have the best chance of thriving.

Arthur Piper
Editor

IRM Virtual Training

*With over 30 years' experience
delivering industry-leading
training courses*



There's never been a better time for organisations and individuals to invest in staff development and help the economic recovery post Covid-19.

IRM Virtual Training Courses include:



Fundamentals of
Risk Management



Risk Essentials
Masterclass



Embedding Risk
Management



Risk Reporting



Practical Risk
Appetite & Risk
Tolerance



Risk in the
Boardroom



Risk Culture



NEW Risk Leadership
& Organisational
Diversity

Find out more at:

www.theirm.org/training-mag



Developing risk professionals



10



18



22



28



34

Features

10 Chain reactions
The pandemic is wreaking havoc in global supply chains, yet businesses often fail to have a basic overview of their operations. Greg Schlegel says the time is right for risk managers to take up the challenge

18 Relationship trouble
Before last year, risk managers knew they were living in an interconnected world. The pandemic showed them what disruption to that web of connections really meant. It is time to learn the lessons

22 Quantum effects
The world's interdependence has led to an ecosystem of risks that appear to have quantum qualities. How do businesses manage environmental, social and governance initiatives given this radical uncertainty?

28 Buyer beware
Purchasing software to support governance, risk and compliance management initiatives can be fraught with difficulties. Following four well-defined stages can help steer a clear way to success

REGULARS

7 IRM Viewpoint
At a time when managing risk is at the forefront of every leader's strategic decision making, IRM has appointed a new independent non-executive chair

8 Trending
The stories and news affecting the wider business environment as interpreted by our infographics team

34 IRM Focus
IRM's Innovation Special Interest Group has been exploring how advances in technology is changing what being a risk manager means

36 Directory
In need of insurance services, risk management software and solutions, or training? Look no further than our listings

38 Toffler
With office life potentially opening up in the near future, it may be time to reintroduce playtime at work

The Certificate in Operational Risk Management

The ideal qualification for anyone looking to develop an understanding of international operational risk management.

Get the recognition you deserve. All CORM holders will now be able to use the post-nominals CIOR, the benefits are that it will help to raise awareness of you achieving the qualification, as well as building your professional status within the risk management community. To apply for the designation (once you've passed) you'll need to renew your IOR membership subscription annually.

The international CORM qualification provides students with an introduction to operational risk management including the tools and techniques used and how it fits into the wider risk management of the firm. The qualification is externally accredited at RQF Level 4/EQF Level 5, and is ATHE regulated by Ofqual.

Risk professionals have never been so busy and pivotal to the survival of organisations of all types globally, risk management has undoubtedly been at the heart of the global response to Covid-19. Our profession is firmly in the spotlight.

What our students say

Justine Keys

HR Risk Manager, Risk & Regulation – Human Resources at Santander UK

"The IOR CORM has given me a comprehensive view of the fundamentals of operational risk management. This has enabled me to better understand how we manage risk within my own organisation and add value in my role as a Line 1 operational risk manager in the HR function."

Ellis Williams

Consultant – Financial Crime at National Australia Bank Limited

"CORM has added real value to my self-development and potentially career opportunities by providing me with a working knowledge of a subject that I had limited prior exposure to. The course content was complemented by real-life examples to illustrate operational risk concepts providing for a much better appreciation of the subject and its implications."

Find out more at:

www.ior-institute.org/corm

IRM appoints new chair

At a time when managing risk is at the forefront of every leader's strategic decision-making, IRM has appointed a new independent non-executive chair

IRM has appointed Stephen Sidebottom, former global head, business HR, at Standard Chartered Bank, as its new independent chair. Iain Wright, CFIRM, has stepped down.

"I'm delighted to take on the role of chair of the IRM at this important point in its growth, Sidebottom said. "The Institute is at an exciting time in its history, where we can look forward and really make our mark."

He said IRM would be increasing the diversity and content of its product portfolio, in both qualifications and training. And he said that he was particularly keen to see IRM continue to operate in global markets and expand internationally.

Risk at the forefront

"Over the last year, managing risk has been at the forefront of business leaders' minds, and as we start to come through the COVID-19 crisis, IRM has a unique opportunity to use its outstanding expertise in risk management to strengthen the role of professionally qualified risk managers in addressing future risks," he said. "As the pre-eminent global risk management institute, I believe IRM is ideally placed to champion the debate



about the skills and risk management approaches that risk professionals and organisations need to succeed."

He said that during Wright's term as chair, IRM had gone from strength to strength.

"I'm looking forward to continuing his good work and playing a key part in professionalising risk management globally," he added.

Digital developments

"Stephen is eminently qualified to lead the board into the next phase of the Institute's journey where we can grow in the post-pandemic world," Iain Wright, CFIRM outgoing chair, said. Wright said that almost one and a half years of his time as chair had been dominated by IRM's reaction to COVID-19, and he was very pleased how the staff, led by chief executive Ian Livsey, had moved

“IRM is ideally placed to champion the debate about the skills and risk management approaches that risk professionals and organisations need to succeed

Stephen Sidebottom, MA, MBA, Chartered FCIPD, FRSA, took over the reins on June 1 this year from Iain Wright, CFIRM, chief risk officer, Europe, Canada Life. Sidebottom has over 30 years' international experience of working in HR and organisation development primarily in global financial services and in both private and public sectors. He also has nearly 20 years' experience on the boards of various membership associations.

IRM into a position where it was fully able to deliver qualifications, exams and training remotely.

"Despite the pandemic, IRM is better placed than ever, and we are now at a point where we can take advantage of those digital developments and our financial strength to start on the next phase of our journey to consolidate our position as the world's leading body for enterprise risk management," he said. 

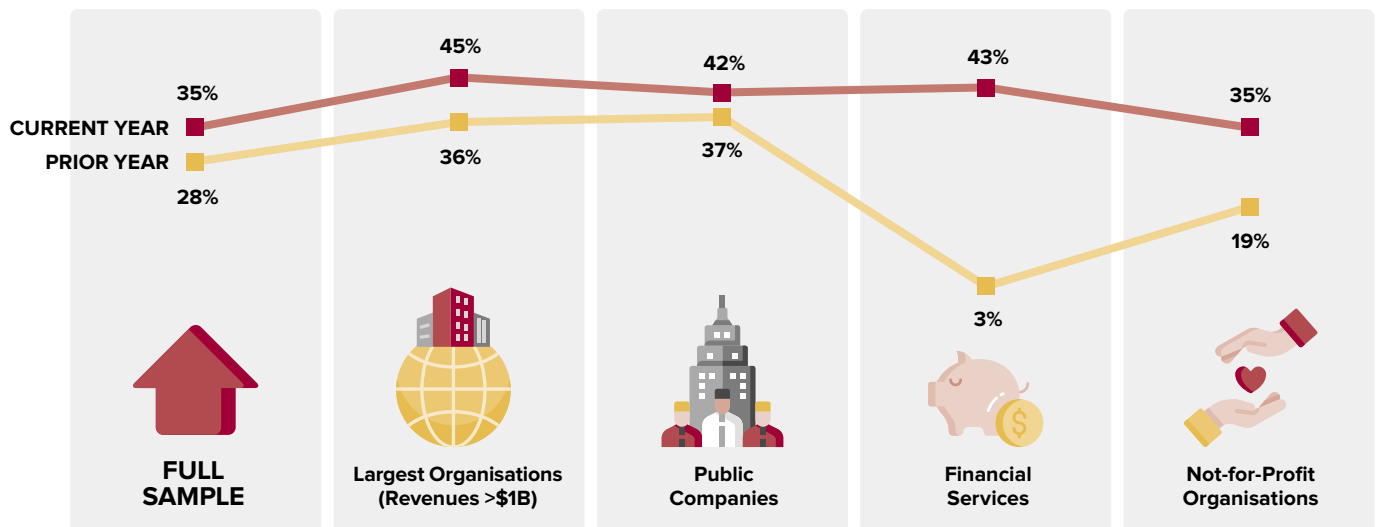
The latest stories and news affecting the wider business environment as interpreted by our infographics team

Jump in demand for risk management information

Many organisations are experiencing an increased demand for better risk disclosure from outside the business

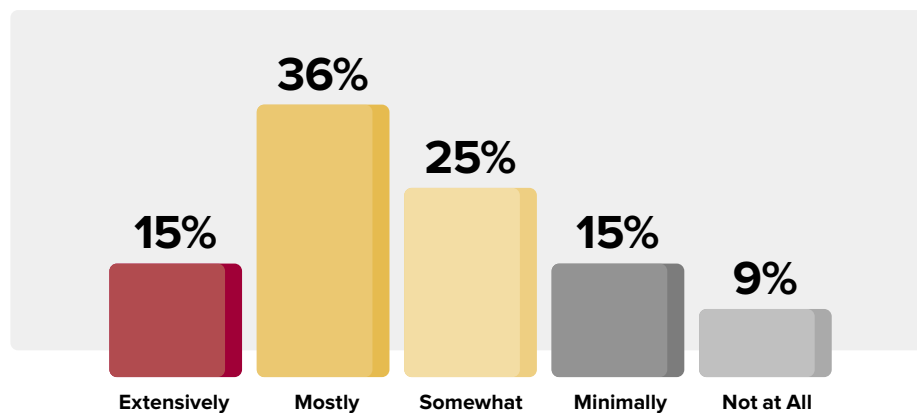


Extent that external parties are “mostly” to “extensively” applying pressure on senior executives to provide more information about risks affecting the organisation:



But too few ERM systems focus on emerging risks

Extent to which the organisation’s ERM process formally identifies, assesses and responds to emerging strategic, market, or industry risks:



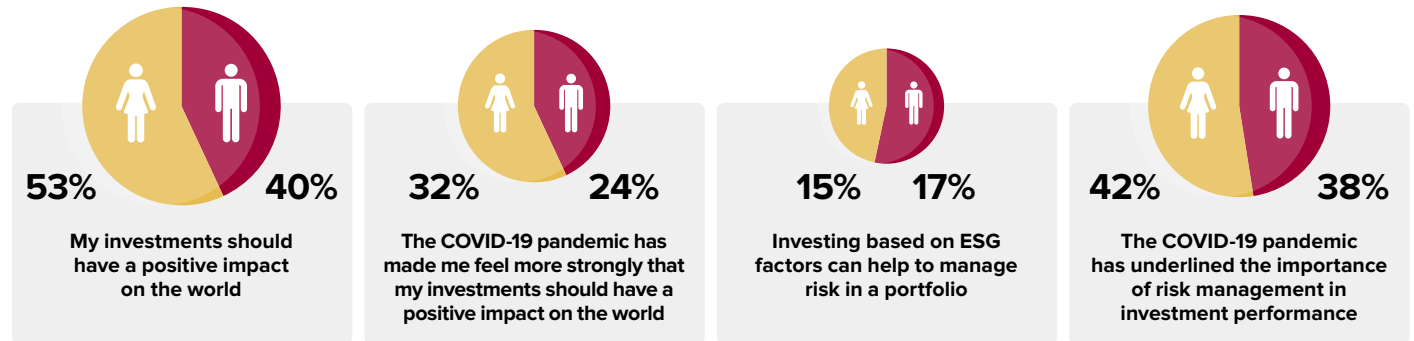
Source: *The state of risk oversight, an overview of enterprise risk management practices 2021*. NC State, Poole College of Management

Investors swing to environmental and social governance issues

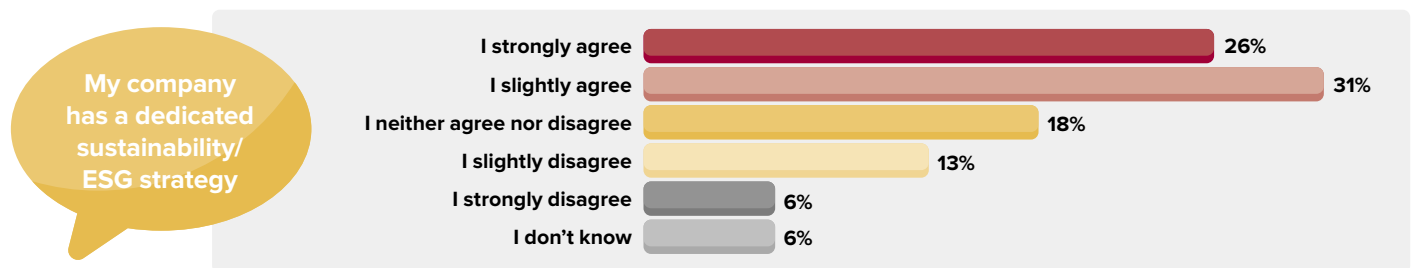


Women mostly lead the way in swing to more ethical outlook

(Figures show percentage out of each question that strongly agree with those statements)

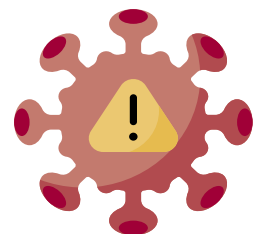


But only just over half of companies have a proper ESG strategy

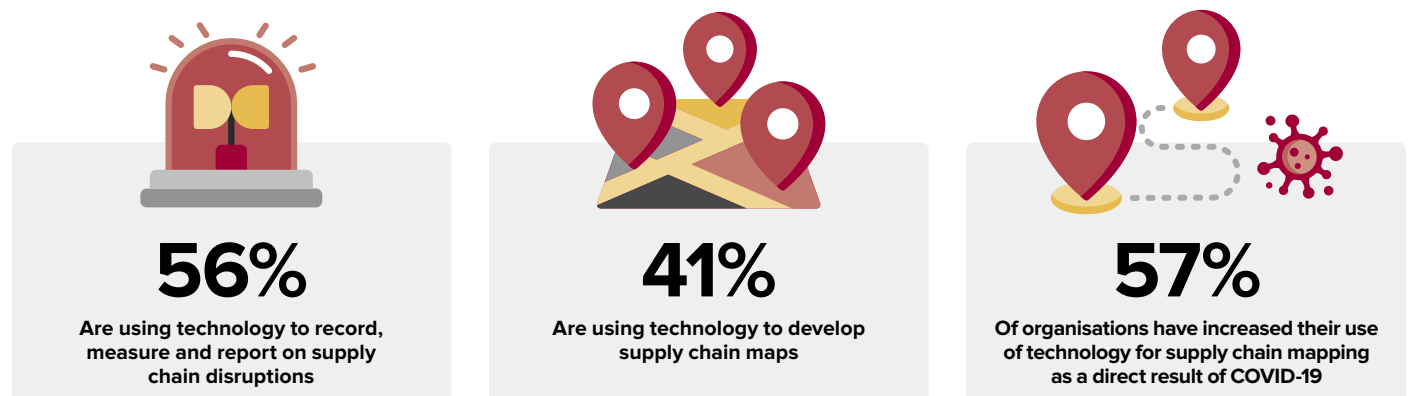


Source: CIO Special, Biodiversity loss: recognising economic and climate threats, Deutsche Bank Chief Investment Office.

Covid-19 moves technology centre stage in supply chain risk management



For the first time, more than half of organisations are using technology to help record supply chain disruptions



Source: Supply chain resilience report 2021, BCI.



Chain reactions

BY ARTHUR PIPER

The pandemic is wreaking havoc in global supply chains, yet businesses often fail to have a basic overview of their operations. Greg Schlegel says the time is right for risk managers to take up the challenge

In supply chain risk, time is money. The long delays at the UK border in January this year and the ongoing saga of the container ship *Ever Given*, which was stuck during April in the Suez Canal, are just two recent examples of how disruptive breaks in those chains can be.

Companies did know that Brexit would cause delays and have known for years that the Suez Canal is narrow. The problem is that too many have a poor grasp of the complexity of their supply chains. “Most companies – small, medium or large – do not have good supply chain visibility,” Greg Schlegel, founder at The Supply Chain Risk Consortium, in New Jersey in the United States, says. And even where they have mapped their suppliers, they still



have more work to do.

“Good visibility means, upstream, understanding who your suppliers are and what is going on with them, and, downstream, what is happening to your customers,” Schlegel says. “Everybody in this

discipline starts with suppliers because they assume that is the riskiest area, because they don’t directly control them,” he says. Risk events downstream, such as a fire in a warehouse, can also have a serious impact on the business’s ability to operate. “Having this complete visibility is crucial for a simple reason: “What you don’t know about your supply chain can and will hurt you,” he says.

Pandemic

The pandemic has been a global testing ground for supply chains, but most businesses have been



**What you don't know
about your supply chain
can and will hurt you**



In risk management, speed is life

too busy struggling to survive to notice. The pandemic has created extra pressure on businesses to become more cost-effective, guard revenues and ensure that they have enough cash flow to survive until lockdowns ease. Often, the first time they know they have a supply chain problem is when disaster strikes, or demand fluctuates unpredictably because of rapidly changing customer buying habits or spikes in pandemic-induced needs.

Over the past year, for instance, there have been shortages of semiconductors, toilet rolls, vaccine ingredients and protective medical equipment – to name just a few. Even the best practitioners of supply chain risk management are struggling to cope with supply shocks and out-of-the-blue government restrictions, he says.

For those who may be sceptical about the importance of supply chain risk, Schlegel is equipped with a worrying array of statistics. Multiple studies show that where regions have been hit with natural disasters – floods, earthquakes, devastating fires, virus outbreaks – around 20 per cent of businesses collapse within 12-15 months. He sees the pandemic as a natural disaster the impact of which has yet to play out. “Take that 20 per cent and apply it across the entire globe – that is what is happening,” he says. “During the pandemic, during the lockdowns and after – and we haven’t seen the after yet.”

Even in normal times, many companies suffer about one risk event per month to their supply chains. A survey last year by the analyst GEP, for instance, calculated that European and US

global companies may have lost as much as \$4 trillion through supply chain disruption in 2020. While about half reported that COVID-19 had “significantly” disrupted supply chains, businesses said their supply chains had also been hit by cyberattacks (36 per cent), commodity price fluctuations (33 per cent) and diverging regulations (32 per cent).



By Schlegel’s analyses, an average company spends about \$4 million per year on identifying, assessing and mitigating supply chain risk. He does not calculate the numbers just for fun, but first started using them as a lecturer with his MBA executive students at Lehigh University (where he is executive in residence in supply chain risk management), who are



taught to make decisions based on Key Performance Indicators. “The minute you have the dollar value of the cost of supply chain disruption, risk managers can show what they are doing to mitigate that – and can calculate a hard return on investment going forward for their risk activities.”

Getting a grip

The costs are high often because companies are too reactive to supply chain risk. They have poor visibility of routes to both suppliers and customers, so when a risk arises, they are caught off guard. “If as a risk manager you do nothing else, you need to improve your supply chain visibility upstream to your suppliers – and downstream to your customers in terms of communication – preferably electronically,” he says. While he acknowledges moving onto cloud-based services presents its own set of potential threats, risk managers can use

their expertise to identify, assess and mitigate those before moving over to those systems. But if the business is too risk averse for the cloud, it could be sacrificing the type of transparency in its supply chains essential for survival. In addition, a proper digitised supply chain also enables the risk team to do sophisticated scenario planning – asking the kind of “what if?” questions that can help when disaster strikes.

Taking a global approach to supply chain risk management is also vital, he says. He is a big fan of risk alert solutions from specialist software organisations. These provide up-to-the-minute risk assessments every half hour or so to their subscribers. “In risk management, speed is life,” he says. “If you can identify a risk, assess that risk and mitigate that risk faster than your nearest competitor, that is a strategic advantage.”

These two steps constitute

the first commitment to risk management in the enterprise, he says, the beginning of a journey from awareness to education across the entire enterprise. “You need to understand best practices so that you can quickly identify a risk in your supply chain, you can assess it using a protocol or methodology, and, third, the hardest part, mitigate the risk,” he says.

Risk managers can learn such risk mitigation tactics through study, initially. That could include taking specialist qualifications, such as IRM’s Certificate in Supply Chain Risk Management, which Schlegel’s Consortium helped create using its own huge array of knowledge as supply chain professionals and tailoring it to enterprise risk methodologies. But applying mitigation tactics in the real world is a challenge.

“Identifying your risk and assessing your risk is what we call an academic exercise – there is



no action, or reaction there,” he says. “I can do that as a professor and list them in descending order of likely impact and tell you how much money is at risk. I go home and the company does nothing. Sadly, it happens.” Mitigating risk is much more difficult because it involves people in the business taking real action and altering their behaviour, changing their usual working methods.

Altering behaviour

To alter behaviour in the business, risk managers may need to change their own approach to communicating their findings and recommendations. Backward-looking analyses of risk, for example, are unlikely to persuade the executive team that change is needed. Heat maps decked with traffic lights or risk integers ranging from one to five can be equally ineffective, he says. “If you advocate and use metrics, methodologies and reporting to the board that is forward-looking and provide the assessment in terms of dollars and cents, we feel you have a higher probability of gaining traction.”

To successfully identify, assess, mitigate and manage supply chain risk, risk processes need to be embedded into daily business decision-making. He accepts that while the word embed is easy to grasp intellectually, it is difficult to implement in practical terms. In the US, he says, Coca-Cola has been an exemplar for supply chain risk management for years. Not only did it have three directors tracking supply chain risk globally, backed up by risk alert companies, they also mapped and embedded risk processes throughout all of its regions.

One of the key tools the company developed was an interactive and dynamic risk register – very unlike the static models that have been the target of critics over the past few years. Instead, at Coke, every management team in the 160 countries where it operates could search and update it in

real time. Let’s say there was a water-borne risk event in New York City. The US team searches the database and identifies a similar event in Kenya from the previous year. They contact the Kenyan team, talk through the mitigations and try to improve on the effectiveness and timeliness of their response. The risk register is updated with their mitigation response plan so that the events are linked and searchable by anyone else in the organisation.

“That is one of the best approaches to embedding risk protocol into your daily lives,” he says. “We would advocate that when it’s the right time, you

Think big in supply chain risk – start small and implement quick

probably should buy or build a dynamic risk register and get it into the daily lives of people other than a risk professional. It is a critical success factor.” Another is to train and educate frontline people so that they can own the risk, rather than simply gathering knowledge in a centre of risk excellence.

To make such changes, the risk team needs funding – that can be a challenge. But presenting the risk factors in hard currency can help make the argument. Initiating cultural change is also difficult. Schlegel says that creating small initiatives in a specific part of the supply chain process that can demonstrate return on investment is a good idea.

“Get a sponsor – executive cover and funding – and do a proof of concept to show how that methodology will improve the bottom line,” he advises. “Think big in supply chain risk; start small and implement quick.” When the executive team is intrigued, try to link successes to how badly competitors fared by comparison. A feature of the

pandemic has been precisely this sort of competitive behaviour in supply chains, he says – who gets online faster and better has been important.

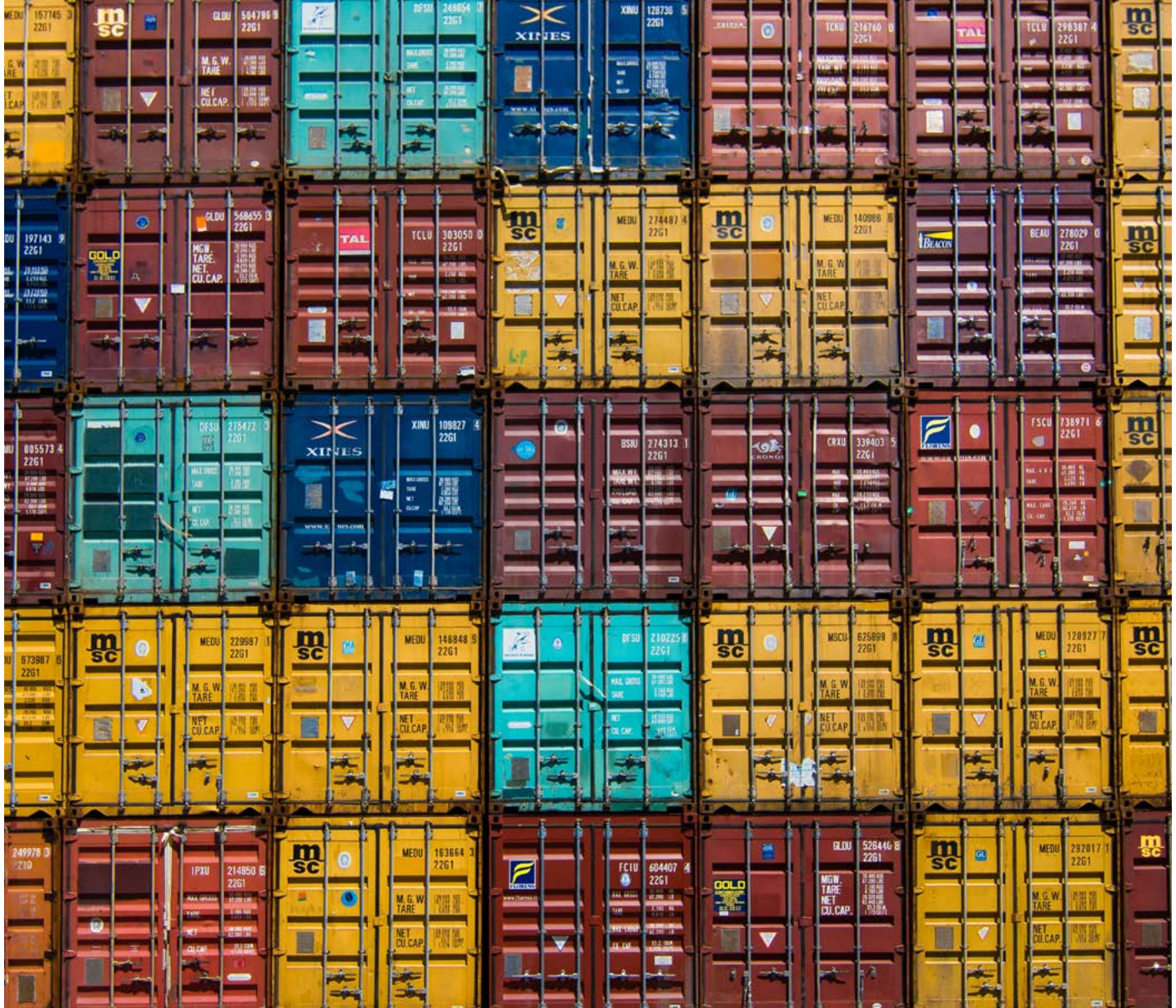
Giving back

Schlegel got into supply chain risk management almost by accident. Having worked for 30 years in supply chain management at US Fortune 100 global companies, he decided to give a bit back and teach. He started at Lehigh in 2010, teaching business undergraduates the basics of supply chain management. During the second term, he was having lunch with the faculty dean and director and

they were talking about supply chain disruptions that were hitting the news. They felt that graduate MBA students really needed to know about such risks. Schlegel was asked to design a 42-contact hour MBA class that all students had to take if they majored in supply chain management.

Schlegel accumulated and codified all the articles he could find and created a course. It was so well-received that he agreed with Lehigh to build a consortium as an incubator, effectively a university spin-off. Starting with five to six organisations, with Lehigh as a longstanding member, it now comprises about 30 companies and 1,500 supply chain professionals. There is a book, courses and events – and now a partnership with IRM that has helped create the IRM SCRM Certificate.

From Schlegel’s perspective, there is a broader relevance to his partnership with the Institute. “We have our own courses, but IRM’s audience is totally different,” he says. “ERM professionals. Our audience is chief operating officers, vice-presidents of supply



“ We would advocate that when it’s the right time, you probably should buy or build a dynamic risk register and get it into the daily lives of people other than a risk professional

chain and so on. But we would love in the future to see more dialogue between the two big, powerful groups in every company – finance where chief risk officers reside usually, and the other powerful group for manufacturers, which is operations and supply chains. If you get those two disciplines talking the same taxonomy, that is a strategic advantage.”

He is keen for younger people to get into supply chain risk management by starting with IRM’s SCRM Cert. Getting an education is important. But he also sees the discipline as new, unlike general risk management. That means there are opportunities for those who learn the identification assessment and mitigation approaches and

start connecting with people on platforms such as Facebook and LinkedIn. “The minute you start to engage with other folks outside of your risk environment and you are adding value to a problem or an issue that a chief executive officer has, you are building a brand, gaining traction and street credibility,” he says.

As the world continues to struggle with the ongoing effects of the pandemic, supply chains are likely to be under unprecedented strain. Not all businesses will survive – and not all risk managers will add the value their organisations need. But those that do are likely to be in an excellent position to grasp the opportunities that are sure to arise out of the wreckage. ☞

Supply Chain Risk Management Certificate

Identify, analyse & prevent

Our Supply Chain Risk Management Certificate will help businesses build resilience in their supply chains. Study online from anywhere in the world with practical learning outcomes that can be put into practice to benefit your organisation immediately. The specialist certificate is awarded by the IRM and developed with support from the Supply Chain Risk Management Consortium. The qualification provides a broad understanding of supply chain risk management principles and practices.

By the end of the qualification, you should be able to:

- Identify, assess and control the supply chain risks that your organisation faces
- Demonstrate an understanding of how supply chains operate and the risk implications of ongoing developments
- Contribute to supply chain financial risk transfer decisions

What our experts say



Robert J Trent PhD

Professor of Supply Chain Management, Lehigh University

"Far too many companies gain an appreciation of supply chain risk only after suffering directly the adverse effects of risk. This certificate provides people with the knowledge, concepts, and tools to enable them to become a valuable part of their organisation's efforts to survive and prosper in an ever changing world."



Nick Wildgoose

Independent Supply Chain Risk Consultant

"There are supply chain disruption and reputational incidents happening every day, that could have been better managed to drive value. This new qualification will help learners develop a clear understanding of supply chain risks, and the tools and technology which can help organisations stay protected."

In collaboration with

SUPPLY CHAIN RISK MANAGEMENT
CONSORTIUM™

Find out more at:

www.theirm.org/scrm-mag

Resilience, risk and recovery





Relationship trouble

BY MICHAEL RASMUSSEN

Before last year, risk managers knew they were living in an interconnected world. The pandemic showed them what disruption to that web of connections really meant. It is time to learn the lessons



Martin Luther King Jr stated: “Whatever affects one directly, affects all indirectly. I can never be what I ought to be until you are what you ought to be. This is the interrelated structure of reality.” This statement is true in our individual relationships, and it is true in an organisation’s relationships in the extended enterprise.

That is because the structure and reality of business today has changed. It is not the same as it was a few decades back. Bricks-and-mortar walls do not define today’s business, nor is it defined by traditional employees. The modern organisation is supported by an interrelated structure of business relationships. It is an interconnected and interdependent web of suppliers, vendors, outsourcers, service providers, contractors, consultants, temporary workers, brokers, agents, dealers, intermediaries, partners and others. Business today relies and thrives on third-party relationships; this is the extended enterprise.

Governance

The business’s ability to reliably achieve corporate objectives directly depends on the governance of third-party relationships and whether the organisation can reliably achieve objectives in each relationship. The organisation’s ability to manage uncertainty, risk and resiliency requires that risk be managed in third-party relationships. The integrity and ability of the organisation to comply with regulations, commitments and values are measured by the integrity of its relationships as well.

The saying “Show me who your friends are, and I will tell you who you are” translates to business: show me who your third-party relationships are, and I will tell you who you are as an organisation. The modern business depends on, and is defined by, the governance, risk management and compliance of third-party relationships (third-party GRC) to ensure the organisation can reliably achieve

pandemic that shut down the world and its various borders. Then, racial tensions and a focus on discrimination led to re-evaluating conduct rules within the organisation and across relationships – followed by more wildfires in California, disrupting businesses. And the year concluded with significant political turmoil, controversies and a major security breach in a third-party context for the



The integrity and ability of the organisation to comply with regulations, commitments and values are measured by the integrity of its relationships

objectives, manage uncertainty and act with integrity.

Third-party GRC is in a state of growing maturity and evolution. The year 2020 has brought many third-party management lessons through the trials and tribulations worldwide, and as a result, 2021 is aiming for greater resiliency and integrity in risk management, resiliency and integrity in the extended enterprise.

What we learnt in 2020

We cannot understand the 2021 trends in third-party GRC without understanding what transpired in 2020. The last year has taught organisations many lessons in third-party management which provides the foundation for the 2021 trends.

Last year brought organisations disruption that impacted operations and third-party relationships. What started with devastating wildfires in Australia moved into a global

history books with the SolarWinds breach. The year 2021 has shown us further disruption because of COVID-19 resurgence in some areas, restriction in supply chains, shortage of shipping containers and the delicacy of supply chains with the Suez Canal incident.

A risk event has a domino impact on the organisation and its relationships. What starts with one domino of risk has a cascading effect on other risks. Consider the global crisis and pandemic of COVID-19. It began as a health and safety risk coming out of Asia. It then had a cascading influence that caused other risks to materialise, and ultimately that impacted the organisation and its third parties. Third-party risk cannot be managed in isolation but must be understood in the complex web of interconnections of risk and objectives that play out from it (see *The pandemic’s web of interconnected risks*). What originated as a health risk



THE PANDEMIC'S WEB OF INTERCONNECTED RISKS

- 1 Risk to objectives.** As the pandemic unfolded, it had a specific impact on business objectives that impacted third-party relationships' objectives. Adapting to the crisis, businesses had to modify corporate objectives and, as a result, objectives in each relationship.
- 2 Risk of operational resilience and continuity.** Organisations have increased exposure to their operations and delivery of business processes across third parties. There were significant issues where service providers and outsourcers entirely shut down because of lockdowns and were unable to support organisations and deliver services, including constrained supply chains and the inability to deliver goods. Outsourced data centres went dark with a skeleton crew of staff to maintain them, often remotely.
- 3 Risk of information security.** With the focus on supporting a broad work-from-home strategy for both employees and third parties, the organisation faced increased exposure to IT security issues. With the Internet of Things (IoT), the light switch, blender or TV in the third-party employee's home could be a source of exposure to company data and connections.
- 4 Risk of integrity, culture and control.** With rapidly changing processes to address the pandemic, the organisation lacked controls to monitor third-party relationship changes. With reduced staff, employees in third-parties were wearing multiple hats and may not have been properly trained to service the organisation. Working from home offices and not in a corporate building contributed to a culture of insecurity for many.
- 5 Risk of bribery and corruption.** Constrained supply chains and pressure to meet objectives increased the risk of fraud, bribery and corruption. With customs, imports and exports coming to a crawl in some countries, and borders shut down, there was greater corruption risk. Heightened exposure to such corruption means that someone may use a third party to influence a foreign government official and bribe them to expedite their goods over others or to get specific contracts or permits at a time when not much is being done.
- 6 Risk of modern slavery and abuse of human rights.** There was great unrest regarding human rights worldwide; what was an issue prior to the pandemic has only been exacerbated further because of the pandemic. But it goes beyond civil rights and treatment of ethnic groups; it also extends into our facilities and supply chains. The pandemic hit certain areas of the world hard. Factories have lost employees to illness and death. As a result, there has been increased staffing with child or forced labour alongside poor and unwanted working conditions.

in a community in Asia now has a global impact that goes far beyond just an illness.

The years 2020 and 2021 (so far) have been a poster child for business and third-party disruption. They have taught organisations that to reliably achieve objectives, manage uncertainty and act with integrity requires a 360° view of third-party relationships as they serve the organisation. This requires an enterprise view of third parties to monitor the interconnections and impact of uncertainty on objectives.

What can be expected next

The world of business in 2021 is distributed, dynamic and disrupted. It is distributed and interconnected across a web of relationships. It is dynamic as business and relationships change day by day. The ecosystem of business relationships is complex, interconnected and requires a holistic, contextual awareness of third-party risk, rather than a dissociated collection of processes and departments. Change in one area has cascading effects that impact the entire ecosystem.

This interconnectedness of business is driving demand for 360° contextual awareness in the organisation's third-party relationships. Organisations need to see the intricate intersection of objectives, risks and boundaries in each relationship. Gone are the years of simplicity in operations. Exponential growth and change in risks, regulations, globalisation, distributed operations, competitive velocity, technology and business data impedes third-party relationships and the business's ability to manage them.

This challenge is even greater when third-party risk management is buried in the depths of departments and operating from silos, not as an integrated discipline of decision-making that has a symbiotic relationship with performance and strategy of relationships.

These elements of distributed,

dynamic and disrupted business are driving significant changes in third-party governance strategies in organisations. In addressing third-party governance, risk management and compliance, GRC 20/20 is observing five strategic trends organisations are focusing on in 2021 and beyond.

Challenges

The first is integrity because the integrity of the organisation relies on the integrity of its third-party relationships. Organisations are re-evaluating their internal core values, ethics and standards of conduct in 2021 and how this extends and is enforced across third-party relationships. This includes a focus on human rights, privacy, environmental standards, health and safety, conduct with others – for example, customers and partners – and security in third-party relationships. Environment, social and governance (ESG) initiatives and regulations are particularly driving this.

Next is resilience because the organisation has to maintain operations amid uncertainty and change. This requires full situational awareness of third-party relationships' objectives

GRC management, which means that the third strategic trend is the governance of relationships. The relationship's objectives and sub-relationships (for example, contracts, service levels and facilities) need to be clearly defined and governed. It is only after a clear understanding of the objectives, and the governance of those objectives, that risk and uncertainty can be managed in the context of the relationship to deliver those objectives. The organisation is going to need to develop a more assertive approach to governance of relationships to ensure greater risk awareness, resiliency and integrity in those relationships.

Fourth, third-party strategies are focusing on a federated approach. Instead of operating in silos of procurement, information security, privacy, compliance, ethics, quality, ESG and more that do not collaborate and talk to each other, the organisation will develop a federated, third-party strategy to manage and monitor the governance of third-party relationships, the risk (uncertainty) and compliance (integrity) within those relationships holistically. Consistency in onboarding,

an architecture that can manage the range of governance, risk and compliance needs across third-party relationships and be able to integrate with ERP and procurement systems and provide robust analysis, assessment and due diligence processes to ensure that objectives are met, while uncertainty, risk and integrity are managed in each relationship.

The end game is that organisations need a complete view of what is happening with third-party relationships. This contextual awareness requires that third-party management have a central nervous system to capture signals found in assessments, and changing risks and regulations for interpretation, analysis and holistic awareness of risk in the context of third-party relationships. 

 **Michael Rasmussen is an internationally recognised pundit on GRC and founder of GRC 20/20 Research, LLC. He is honorary life member of IRM.**

“ Organisations are going to need to develop a more assertive approach to governance of third-party relationships to ensure greater risk awareness, resiliency and integrity in those relationships

and performance in the context of uncertainty and risk within those relationships. Given the reliance on third-party relationships, this requires a holistic view into the GRC of each third-party relationship and how it serves and provides value to the organisation.

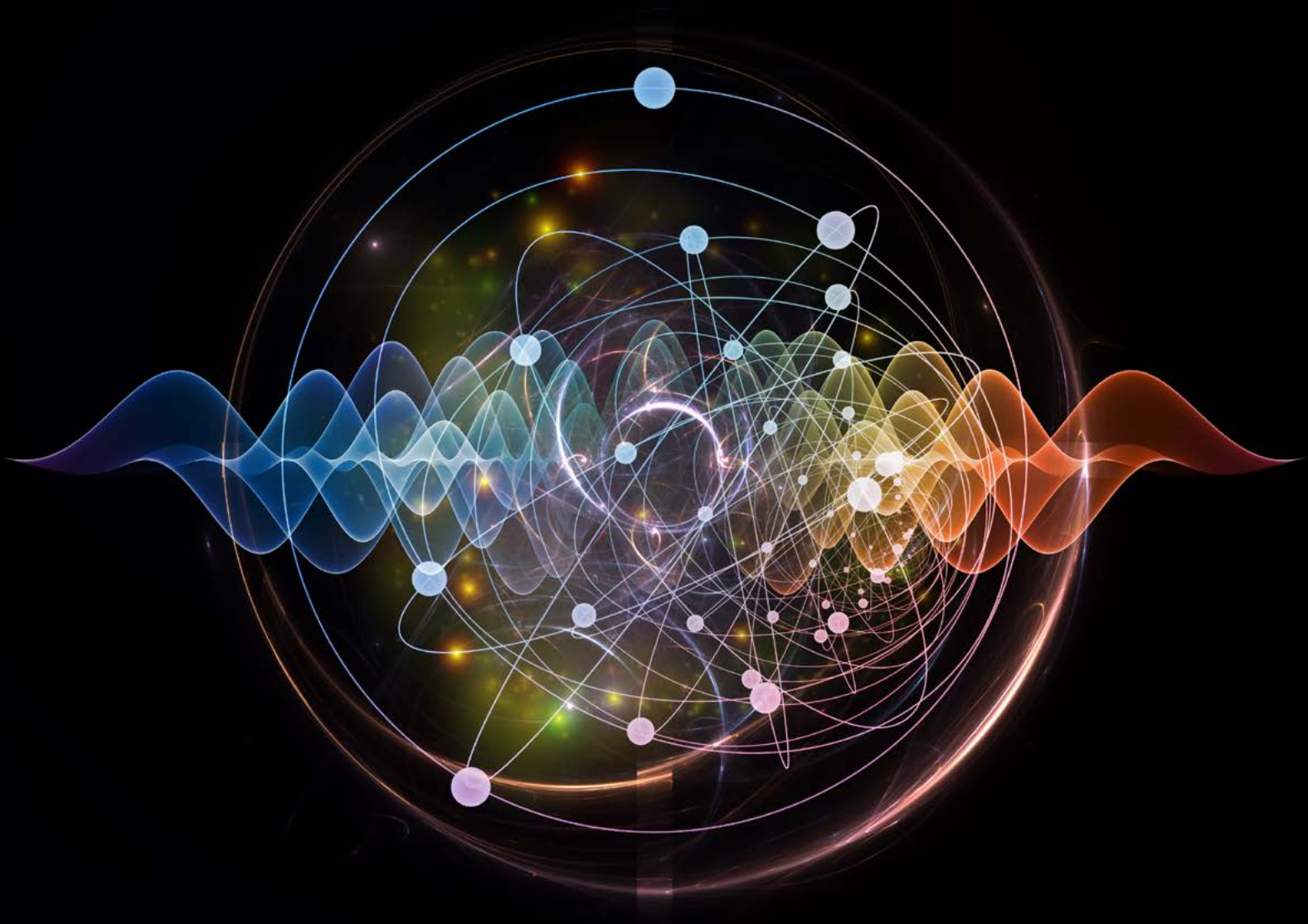
Third-party risk management is not enough. The organisation is shifting focus to third-party

ongoing monitoring, auditing/inspections, incident management, assessments and offboarding will be built across the needs of these collaborating departments.

Finally, integration will mean that to support a federated, third-party strategy, the organisation will look to re-design its third-party technology and information architecture. This will involve

Quantum effects

BY PEADAR DUFFY



The world's interdependence has led to an ecosystem of risks that appear to have quantum qualities. How do businesses manage environmental, social and governance initiatives given this radical uncertainty?

Money is pouring into environmental, social and governance (ESG) initiatives, investing and reporting. The value of global assets applying ESG data to drive investment decisions has more than tripled over the eight years to 2020 to \$40.5 trillion, according to the research firm Opimas. The *Financial Times* recently reported that ESG funds would outnumber conventional funds by 2025. But why?

A combination of factors, but no doubt including COVID-19 awakening our collective sixth sense that Mother Nature is not too happy. There is also enlightened self-interest on the part of capital markets arising from the prospect of traditional business models collapsing over the next decade. While we all have a vested interest in saving the planet and ensuring strong economic growth over the longer term, the capital markets matter more than we do for two big and basic reasons. They have the money, and we do not. Investment funds invest people's savings with a view to sustainability over longer-term returns on those savings.

Herein lies heavily regulated fiduciary undertakings, which are fulfilled in a number of ways, addressing the long-term benefits of future generations. A long-term return is clearly dependent on sustainable growth with well-

functioning markets and good corporate governance. And ESG issues are drivers of long-term risk, long-term return or both. For example, business resilience and long-term financial performance is determined by detecting investable signals gleaned from monitoring how well management

“ We all have a vested interest in saving the planet and ensuring strong economic growth over the longer term

are doing managing transition (to Net-Zero) and long-term ESG issues and opportunities. Metrics are proven to be material to a company's long-term operations and performance.



America's race to zero emissions
<https://bit.ly/3w2Frq3>

Three dimensions

There are three principal dimensions to the ESG risk landscape for risk professionals

today. First, confusion exists given the alphabet soup of global ESG standards which abound. The good news, however, is that we can expect significant improvements in the near term with much work being done to coalesce principal standards. This will help focus resources and improve the quality of disclosures made by companies. With some 80 per cent of S&P 500 valuations attributable to intangible assets we will shortly see the arrival of “integrated financial and non-financial reporting.”

Second, the quality of third-party ESG ratings and performance analyses is uneven. Pressure on boards to demonstrate pathways to Net-Zero has accelerated the practice of alchemy. Specifically, generating mathematised numbers, in the form of ESG ratings, to accurately reflect what is deemed to be material – that is, what really matters to companies across particular industry sectors. The challenge with this approach is that people can find themselves generating plugged numbers and statements. By this, I mean numbers and statements with no drill-down to source data and which therefore cannot always be independently verified and audited.

Finally, the reliability of ESG risk data provided by companies themselves remains the most complex challenge. Why? ESG pertains to all of the non-

“ Curiously, from this destruction has come new opportunities

financial activities undertaken by companies across all of their operational activities. This translates to different people, using different ESG and operational languages, and different ways of measuring risk.

Does this sound familiar?

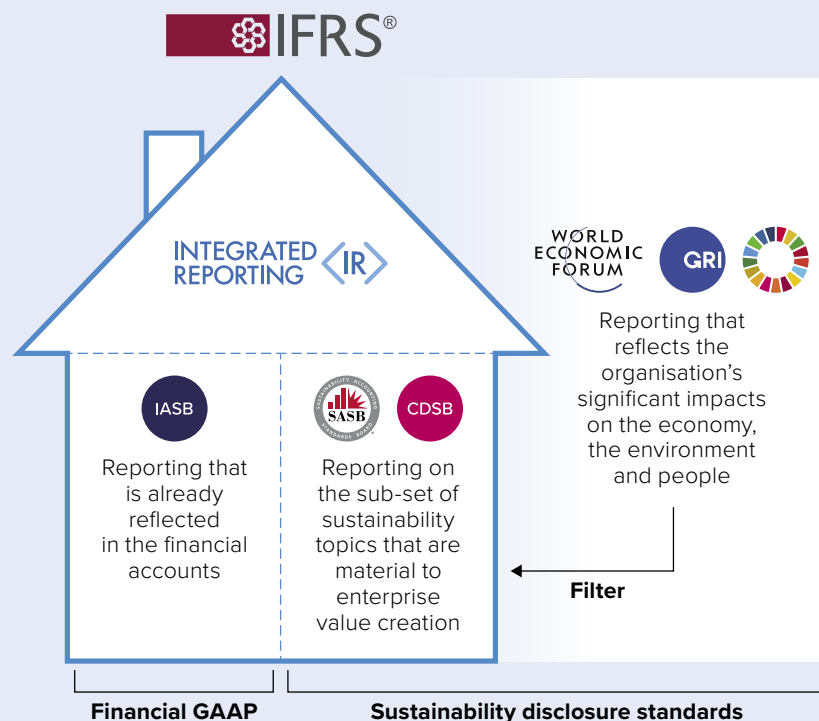
Consider the diagram MIT reports that ESG data is unreliable depicting principal ESG operational challenges. Now add to it supply chain, cyber, privacy, GDPR, anti-slavery and anti-bribery data, for instance, all of which fall under the S of ESG. Add then to that risk governance, and incident and crisis management, which fall under the G of ESG. What do you see? ERM wine in an ESG bottle.

Risk and reward

Risk and opportunity are conjoined – two sides of the same coin. What joins them together is uncertainty – the quality and reliability of information and knowledge with which to credibly inform decisions towards the achievement of objectives. In essence, anything which can accelerate, slow down or obstruct pursuit of an objective is a risk. In practical terms, every time we make a decision, we are managing a risk that things might go up or they might go down, they might go according to plan or they might not.

That is why framing the ESG risk-reward equation requires that we step back momentarily to consider the big picture. Companies are not created to manage risks. They are created to generate value. Whether it is a charity created to generate social good, or a commercial entity created to generate surpluses across all stakeholders, all

A COHERENT, COMPREHENSIVE CORPORATE REPORTING SYSTEM



Source: LaptrinhX.com – IFRS Foundation Aims for Coherence, Not Complexity

entities are created to generate value of one kind or another. Value generation has a natural rhythm to it, the yin and yang of value creation and value preservation. And the decisions we make as we wrestle with both towards the achievement of our organisational objectives is what we call managing risk.

Using risk jargon and looking back, ESG risk has been the proverbial Grey Rhino grazing placidly on the plains over the years – that is a highly likely but ignored threat. It took the form of a steady flow of weather phenomena, SARS, MERS, Ebola and so on streaming across our news channels. But then, to mix metaphors a little, a Black Swan appeared. It took the form of a sudden, previously unimagined thing stopping the global economy. The Grey Rhino was the risk source, the Black Swan the global lockdown we have

being living with for the past 12 months. Curiously, however, from this destruction has come new opportunities where the first dividends already received include new ways of working, accelerated digital transformations (significantly in terms of breaking down human resistance to change) and new technologies from sequestering greenhouse gases to reimaged ways of doing old things in new ways.

Boards intuitively understand that to grow and sustain a business over the longer term we need to risk failure in trying out new things, while nurturing and sustaining the cash cow – while also keeping enough reserves for the rainy day. That is because boards have an appetite for certain types of risks, in pursuit of their value creation objectives. But they also know that to consistently and reliably generate value over time they need an equally robust

MIT REPORTS THAT ESG DATA IS UNRELIABLE

The MIT Aggregate Confusion Project reports significant non-correlation between ESG Raters on ratings applied to organisations... "Our findings demonstrate that ESG rating divergence is not merely driven by differences in opinions, but also by disagreements about underlying data".

E = Environment
S = Social
G = Governance



Source: MIT Aggregate Confusion Project

approach to value preservation. Here it is likely that strategic leaderships will mandate zero-tolerance of any downsides. So, for example, risk can only be a bad thing in quality, safety, security, IT, data privacy and so on, where any deviation from expected results cannot, and will not, be tolerated. The takeaway is that every time we make a decision we are managing a risk towards the achievement of an objective.

Mark Twain

Do multinational corporations (MNCs) know what they know, do they know what they don't know? This simple question has a non-trivial answer which reminds me of one of Mark Twain's quotes:

"It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so."

Today we live in a complex non-linear world where very many

can often be the best of the wicked options and sensing ways forward from there. Hence complexity. In ESG terms, this explains the serious challenges with seeking

“ Pressure on boards to demonstrate pathways to Net-Zero has accelerated the practice of alchemy

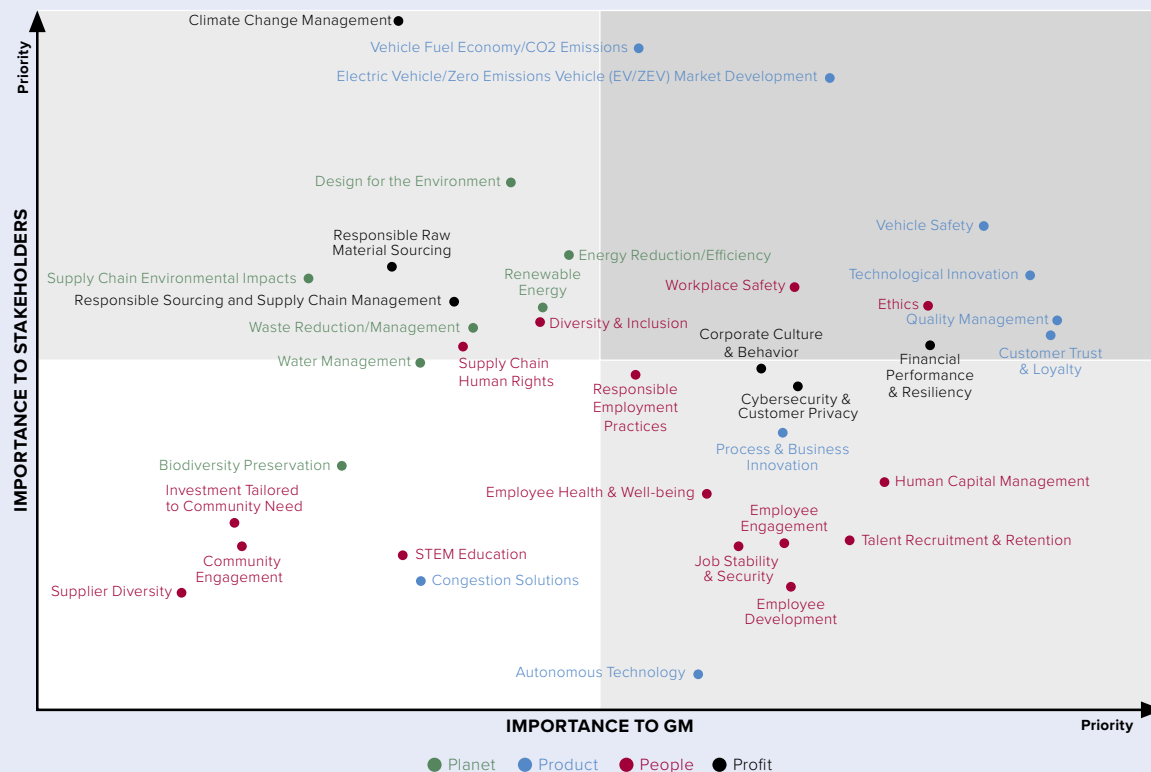
core functions and processes are outsourced or partnered. This gives rise to networked, extended, distributed organisational structures. When things go seriously wrong, the only option

to establish Scope 3* baselines and transition pathways to future state Net-Zero commitments.

At the top of the corporate pyramid, up to 60 per cent of S&P 500 companies will have at least

* Scope 3 emissions are the result of activities from assets not owned or controlled by the reporting organisation, but that the organisation indirectly impacts in its value chain. Scope 3 emissions, also referred to as value chain emissions, often represent the majority of an organisation's total GHG emissions.

GM CASE STUDY – 2019 MATERIALITY MATRIX



Source: A practical guide to sustainability reporting using GRI and SASB Standards

“Quantum risks exist in different states, simultaneously, across systems, yet they cannot be observed together

one physical asset at risk from climate change. The prospect of significant “stranded assets” on the horizon leads to concerns ranging from value deterioration in many cases to value collapse in others. In the middle of the pyramid, there are 60,000 MNCs in the world, which between them directly control 500,000 subsidiaries which in aggregate

account for half the global economy. The rest of the pyramid comprises hundreds of thousands of suppliers contracted by the top and middle of the pyramid.

Over recent decades, globalisation (and profit at all costs) has caused outsourcing of both core functions and core processes across long, fragile supply chains. MNCs today are highly networked and extended across multiple ecosystems. They are comprised of hyper-interconnected, hyper-interdependent complex systems spread across a multipolar geopolitical world growing in uncertainty. This leads to one big and basic fact: MNCs are too big to know what is going on, in and across, their ecosystems.

ESG risks have a massively compounding effect on existing management challenges. How? Whereas international financial accounting does

not require us to report on financial status of suppliers and partners, ESG standards require that organisations report on Scope 3 emissions (under environmental), work practices across our outsourced suppliers (under social) and competent frameworks across both of those that can “demonstrably and credibly” cause the generation of independently verifiable and auditable information.

Not only can organisations not possibly know what they do not know, but now they are required to disclose what they know for sure! So, the key takeaway, to paraphrase Bill Clinton’s quip on the economy, it’s the Ecosystem, Stupid!

When the CFO, sustainability and investment officers ask the CRO for input, do not start with traditional methods, and absolutely do not start generating lists of risks. Step back and



look at the bigger picture. The external and internal contexts. Those interconnections and interdependencies between the internal and extended components of the organisation. Your ecosystem. If you do not know your ecosystem, you will never join the dots connecting what matters most to the achievement of objectives.

The bear in the woods

There is an old saying that when you are running, you do not need to be faster than the bear, just faster than the other guy. This has direct relevance to ecosystem governance.

Ecosystems, digitalisation and pace of technology advancement give rise to a new type of complex risk. A risk which up until recently could not be seen by the naked eye using traditional risk methods and practices. By traditional practices, I mean those practices borne of some decades ago which assumed that all risks could, with a blend of trusted technique(s) and thoughtful consideration, be reasonably identified. Once identified, they could then be assessed and demonstrably credible estimates made as to the likelihood of their occurrence(s). This traditional approach is still sound enough at the level of single entities which are not significantly networked and are relatively self-contained. That is to say they are not part of any ecosystem, the dynamics of which significantly influence the achievement of

their business objectives.

This approach, however, does not work at the level of MNCs where the norm is to have quantum risks. That is, you have risks, which exist in different states, simultaneously, across systems, yet they cannot be observed together. The important thing to understand about these risks is that they are borne of ecosystems, and the more complex and dynamic the ecosystem the more difficult they are to identify. They are particularly difficult to identify and assess unless you know how to track and trace them using advanced technologies and agile risk practices.

The governance challenge is huge as the nature of ecosystems is that MNCs only have jurisdiction over those they control directly, and only the power of enquiry over those which whom they have good contracts. The solution lies in a governance approach to ecosystem-level transparency directed towards sensing and anticipating faster than your less adaptive competitors who will get eaten by the bear. ESG risks are clearly quantum risks. They are borne of your ESG ecosystem, of which you have low to no visibility.

The takeaway here is that ESG risks are quantum risks which constantly traverse ecosystems. They are not static, and to see them you need to be able to dynamically monitor your ecosystems. Everything described above can be done reliably, effectively and affordably. It is not a technology challenge, as such, but a challenge in reimagining new ways of doing old things.

Practical steps

I was reviewing *A practical guide to sustainability reporting using GRI and SASB Standards* published in April 2021 and noted its excellent case studies. One artifact included a materiality matrix which contained nearly 40 discrete ESG topics across people, profit, planet and product. It immediately struck me that for



A practical guide to sustainability reporting using GRI and SASB Standards

<https://bit.ly/3w31vAU>

all intents and purposes it could just as easily have been an ERM matrix, all be it with environment and social centres of gravity.

These kinds of visualisations of what matters most to an organisation can be dynamically linked. First, they can be linked to company objectives where they are tagged to those primary and secondary objectives which underpin performance, as well as other attributes. And they can be linked to company ecosystems so that you can join the dots with actionable insights jumping straight off the screen.

However, I would say, particularly to those running committees directed towards answering multiple ESG questionnaires and getting out big 80- to 100-page ESG reports, that they should start small and start smart. Pick two or three things that matter most to your organisation today and work on those. Find automations which facilitate fast, effective and reliable communications across your ecosystem, starting with a small part of your ecosystem first. It is as simple and as complex as that. 🌐



Peadar Duffy is founder director of SoluxR which is an ESG Risk as a Service (RaaS) provider and a member of IRM's Innovation Special Interest Group.

Buyer beware

BY JIMI HINGHLIFFE AND ARIANE CHAPELLE

Purchasing software to support governance, risk and compliance management initiatives can be fraught with difficulties. Following four well-defined stages can help steer a clear way to success

Firms are increasingly investing in specific software applications to support governance, risk and compliance (GRC) management activities. However, selecting the right GRC system for any organisation and then implementing it successfully is a significant undertaking.

There are four key phases, which we will examine in this article: preparation, selection, implementation and utilisation (see *GRC system: phases, rules and pitfalls*).

Preparation

First of all, risk managers need to have realistic expectations. A GRC solution is not a solution to risk management issues; it is only a tool that operates the organisation's framework more efficiently. It will not do risk management, only support it. Therefore, it is crucial to have a stable and explicit operational risk management (ORM) framework before looking for software support.

Risk managers need to stabilise their existing framework first.

In fact, a common mistake is to implement a GRC system without first addressing known weaknesses or gaps in the risk framework. Carefully reviewing the risk framework can help risk managers to make an informed choice for the system.

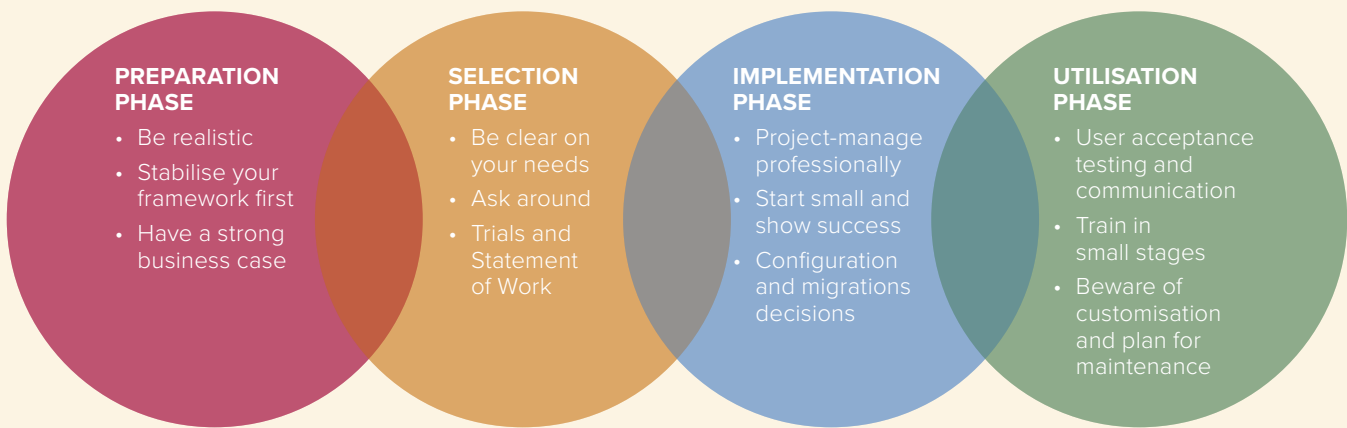
If the ORM framework is underdeveloped or immature, make sure it is set up in a way that is suitable and proportionate to the needs of the organisation. Do this before deciding on software to support the framework because the framework dictates the GRC system that supports it, not the other way around. If the ORM framework has legacies and intricacies that make it too complicated, simplify it. Do not transfer unnecessary complexity to the software. Some firms invest considerable time and money to exploit the immense ability of modern GRC systems to replicate



Some firms invest considerable time and money to exploit the immense ability of modern GRC systems to replicate what they have been doing in spreadsheets



GRC SYSTEM: PHASES, RULES AND PITFALLS



“ We have seen many epic failures where firms have neglected to secure a professional project manager

what they have been doing in spreadsheets. All manner of weird and wonderful ways of doing operational risk are customised into the system, setting in stone a risk framework that may be flawed or over-complicated.

It is also vital to have a strong business case. Every important project needs a clear business plan. Implementing a new – or first – GRC system is no exception. It is essential to be clear on three elements. First, what will the GRC system be used for? If it is just for operational risk, is it only for risk and control assessments, incidents data collection and reporting? Or does it also cover the full scope of compliance, policies and internal audit?

Second, who will the users be? The number of system users and administrators strongly influences both the price and the complexity of implementation. How widely does the business need the first, second and third lines of defence to use the system?

Finally, who will own, maintain and administer the system? Governance and ownership are as important as the technical aspects. Do risk managers want a system that integrates with some or all of the other systems? Who will decide on the interfaces and manage them?

The answers to these questions will influence the next phase.

The vision for GRC systems when they were first introduced was that many business functions would use them, all drawing on the same golden source of data. The reality has been quite different, in large part due to organisational politics. We know firms where risk, compliance and audit were all in the market for a GRC system, but organisational politics led the firms to buy three different systems. A pragmatic approach is to let one function, often the risk one, take the lead and allow other areas to express their views after they have observed the system in action.

Selection

There are numerous GRC systems on the market, which vary considerably in functionality, aesthetics and price, so it is important to be very clear about what you want in a system. If you need the system for risk and control self-assessment, incidents, key risk indicators and producing reports for the risk committee and the board, make sure it has these core functionalities. It is easy to be distracted by other, superficially impressive, functionality that you might never use. Be aware of future regulatory

developments and consider whether additional functionality, such as the current regulatory developments on operational resilience, may be needed.

The important consideration is how well the system meets the organisation's needs in specific areas of functionality. Some vendors provide default content, from risk and control libraries to regulatory handbooks. This can be extremely helpful for firms with immature frameworks. However, if the ORM framework is mature, such content may be of little use. An assessment scorecard may help with selection, enabling risk managers to evaluate the relative merits of each system against

understand what you are buying. Too often, users accept the contract and statement of work without fully reading it and then wonder why they are being charged for things, or why the project went the way it did.

Implementation

Once a system has been selected, it is critical to dedicate enough time and resources to configure and implement it properly. Implementing a GRC system should be treated as a major change programme with senior sponsorship at board level or executive level, depending on the size of the firm. That includes creating a project plan,

than a big-bang approach.

Vendors will rely on the firm's subject matter experts such as risk champions to help configure the system, so they need to be available. Avoid planning a configuration for the summer when many people are on holiday; this can cause project delays, or poor decisions if the right person is not consulted.

The configuration and implementation stages can be extremely challenging if the framework is incoherent or incomplete, which is why all decisions about the design and structure of the ORM framework must be taken before selecting a system. Once the framework is in good shape, the main challenge is to configure the system so that it aligns with the organisation: group structure, entities, functional structure, user profiles and risk framework, including taxonomy, scoring matrices, and risk and control libraries. A proper configuration makes usage far more efficient. For instance, if the organisation is structured vertically by business lines, do not select a system that is essentially process-based, or vice versa.

Deciding whether to migrate existing data to the new system can be a difficult decision that depends on a number of factors, not least the quality of the historical data. If you decide to migrate the data, make sure to complete a rigorous data cleansing exercise only for accurate data suitable for migration. This can be especially challenging after mergers, requiring the mapping of data that may be organised and labelled differently. Recent machine learning techniques can be a great help here.

Utilisation

After configuring the system, ensure primary users complete comprehensive user acceptance testing. Vendors can usually provide checklists for this. Issues, glitches or design changes to the configuration can then be logged. Never shrink the testing



An assessment scorecard may help with selection, enabling risk managers to evaluate the relative merits of each system against the required attributes

the required attributes. Good vendor procurement depends on investigating and reviewing a range of GRC systems – as well as the vendors and teams that will actually work on the project.

Remember that vendors will only provide “gold star” customers as references, so ask around to have a balanced view of customer experience. In addition, be sure to receive a trial version. There is no substitute for experiencing the real thing before you commit, and although it is not quite the same as using the system with your own data day to day, it will give you a fair idea of how the system performs. Make the most of the limited time given by the trial by employing all the trial data and testing users across various functions and user types. Even from the vendor's side, experience shows that the trial is often not used properly.

Finally, before signing a contract, make sure you fully

governance committees and employing all the usual change management disciplines.

Importantly, do not economise on the project manager role: organisations need a dedicated and professional project manager for the whole duration of the implementation. We have seen many epic failures where firms have neglected to secure a professional project manager. Tellingly, some vendors will insist on an internal project manager before they start the project because they know what can go wrong when there isn't one.

Many firms try to implement too much too quickly. Instead, start small with a pilot project, focusing on core functionality and a few departments that can become champions. Look for pilot success stories and proofs of concepts that can be shared with board sponsors. All successful implementations follow cautious and gradual rollouts, rather

“ **Moving from a spreadsheet to a GRC system can be a very different and unfamiliar experience for users**



phase to accelerate rollout, as this would invite disaster.

As part of the testing and the final configuration, ensure there is continuous dialogue between the vendor, the project team and the early adopters. This is key for a successful implementation and utilisation of the new system, as you must achieve a common understanding and purpose.

Training on the system is also key. Prioritise it for the main users, who will need a good understanding of the system to add value to the configuration and the user acceptance testing. After the system is configured, it is time to provide training for new users and answer their questions. Training in small stages is crucial for effective use and adoption. A common mistake is to provide too much detailed training over several days at the start. When users then try the system for real, they may find they have forgotten most of the training. Even with documentation to help them, they might still be lost and will have to be retrained. Moving from a spreadsheet to a GRC system can be a very different and unfamiliar experience for users. Far better that they learn in small stages and only move on

to the next stage when they are comfortable with their progress.

Over-customisation is a trap that many firms fall into. People are often excited about the possibility to customise the system so that it replicates what they are doing in a spreadsheet. Instead of spending lots of time and money making numerous adjustments, it is better to harness the system's inherent benefits. Too much customisation sacrifices these benefits and makes upgrades difficult and sometimes even impossible. Select a system you like, and keep customisation to a minimum.

There must be enough super-users to support and maintain the system. We have seen firms run into trouble when the only person in the risk function who understands the system leaves. Reduce key-person dependency and ensure there is appropriate cross training.

When the system is upgraded – for instance with additional functionality – it will need to be understood by super-users, and users will have to be trained. Most vendors will provide training or “train the trainer” sessions but may charge extra for the service. Most vendors

also run user groups. These are a great way to learn about updates, provide feedback and compare notes with other users. Many vendors also organise user group events and webinars on hot topics, as well as write helpful blogs and white papers. 

 **Dr Jimi Hinchliffe is former chairman of Institute of Operational Risk, England & Wales, and Ariane Chapelle is founder and director of Chapelle Consulting and author of the award-winning *Operational risk management – best practices in the financial services industry*. They would like to thank all the anonymous reviewers of this paper who kindly shared their views and enriched the content with their career-long experience of the GRC world.**



Operational risk management – best practices in the financial services industry

<https://bit.ly/33NAmpy>

Use the code **BPFS2** for a 30% discount to the local list price.

Digital Risk Management Certificate

The essential qualification for tomorrow's risk practitioner



Develop an understanding of risk management in the digital era

The IRM's specialised Digital Risk Management Certificate explores how appropriate risk management tools and techniques can be applied, adapted and developed in the digital context and provides a detailed introduction to cybersecurity principles and practices.

The course covers how to carry out digital risk assessments, provides a detailed grounding in cybersecurity principles and practices and also looks at the ethical issues surrounding both privacy and machine learning.

By the end of the qualification, you should be able to:

- Demonstrate a broad understanding of today's digital technological developments
- Explain how digital technology and innovation is impacting organisations and society
- Contribute knowledgeably to identifying, assessing and controlling digital risks throughout your organisation and its supply chain, associated with new technologies and new ways of working and more

What our students say



Emma Duggan, Risk Manager, Experian, United Kingdom

"The IRM's Digital Risk Management Certificate is extremely relevant to my role and I would urge risk professionals to consider it. It is very relevant for anyone working in technological development, as risk is everyone's responsibility. I have been able to take more of a leading role in ensuring cybersecurity risks are effectively controlled and information security issues are remediated at the root cause."

In collaboration with



Find out more at:

www.theirm.org/digitalrisk-mag

Resilience, risk and recovery



Developing risk professionals

Digital innovation is powering an evolution in risk management

BY SARAH GORDON AND RODRIGO SILVA DE SOUZA

IRM's Innovation Special Interest Group has been exploring how advances in technology is changing what being a risk manager means

Cloud computing, computer-based complexity analysis and artificial intelligence are only some of innovations becoming commonplace in many organisations. The availability of and expectation to use these tools not only requires a step-change in the skill sets required of our risk management teams but also provides an opportunity to evolve how we work.

So, what might some of these changes look like?

Getting the computers to do the grunt work

Very few people like maintaining risk registers. The exciting part of a risk database is the analysis of the content within it. Advances in risk management software allow us to automatically interact with individuals across our

organisations to collect and communicate risk information. They also enable us to more easily store the data in many-to-many datasets. This means

“We are dealing with far larger datasets than ever before

that risk registers enable more advanced analysis without having to spend our lives cleaning and managing data.

We are also dealing with far larger datasets than ever before. Satellites can measure our carbon emissions, procurement datasets provide a network of

trade across the world and the ever-encompassing internet of things amasses huge datasets on our every movement.

“Spiders” comb through our datasets, identifying trends and anomalies that our human brains might otherwise miss.

While these techniques will not give us all the answers, they will help the human risk manager to look at the datasets from different perspectives. It is likely to force us to ask “what if?” in areas where we potentially naively think we are resilient.

This means that the risk manager must become more computer savvy and actively seek an understanding of the possibilities that computing power can offer. We don't need to become expert data scientists, but we need to have a few of these wonderful specialists in our teams.



“ Risk managers must become more computer savvy and actively seek an understanding of the possibilities that computing power can offer

Embracing our own humanity

Empowering our decision-makers to acknowledge and then deal with risks is the core of what a risk manager should be spending their working life doing. If computers can take on the data-crunching work, this frees us up to be more human and become the conscience for our organisation.

To do this, we need to have empathy for those who we work with, see the world through their eyes and understand what they need to make their decisions. We should be able to provide our decision-makers with the knowledge and degree of uncertainty that they need to be aware of in order to balance their opportunities and threats at any particular moment in time.

This means that risk managers need to build trust

with our decision-makers by being charismatic and reliable – despite the uncertainties inherent in our datasets and our knowledge of risks.

Revelling in science fiction

Our requirements as risk managers should also drive innovations in technology. We identify opportunities and threats to be managed on a daily basis. These can be converted into profitable businesses, as has been proven by many of the fintech companies that have emerged in recent years. For some, a perfect world would be one in which we would be able to predict the future. Just because it isn't possible now should not mean that is not a goal we should constantly aim for.

This means that as risk managers we should be prepared to challenge the norm and tell the

world of technological innovation what our pain points are and what we would be willing to pay for.

If you would like to join the discussion on how technological innovation is revolutionising risk management, IRM's Innovation SIG will be running an open online discussion forum on September 29, 2021. Led by a number of inspirational speakers, the purpose of the forum will be to acknowledge opportunities and threats posed to risk management by digital innovation, and what that means for all of us. It would be great to see you there. 

 **Sarah Gordon and Rodrigo Silva de Souza are IRM Innovation SIG co-chairs.**
For more information or to get involved, please contact: membership@theirm.org

Enterprise risk management and risk analysis software



riskHive are an established global provider of professional cloud, intranet and desktop solutions for the management and analysis of RAID (risks, issues, assumptions and dependencies). Being low maintenance, highly configurable and cloud

based, the Enterprise Risk Manager application can get you online in under 24 hours, supporting your existing processes and terminology. Easily import existing risk information to quickly produce a consolidated risk portfolio. Relied on by customers ranging from New Zealand through the Middle East to Northern Europe riskHive deliver a truly global ERM solution with a truly enterprise 'all-in' licence.

 Ian Baker or Doug Oldfield

 +44 (0) 1275 545874

 ian.baker@riskhive.com
doug.oldfield@riskhive.com

 www.riskhive.com

 riskHive Software Services Ltd.
Dilkush, Farlers End
Bristol, BS48 4PG

Governance, risk management, and compliance software



OneTrust GRC enables risk, compliance and audit professionals to identify, measure, and remediate risk across their business to comply with internal rules and external regulations. With OneTrust GRC, companies can seamlessly integrate risk management into their day to day activities. OneTrust GRC is a part of

OneTrust, the #1 most widely used privacy, security and third-party risk platform trusted by more than 6,000 customers and powered by 100 awarded patents. To learn more, visit OneTrustGRC.com or connect on LinkedIn.

 Scott Bridgen

 +44 (0) 7554 515 343

 sbridgen@onetrust.com

 www.onetrustgrc.com

 Dixon House
1 Lloyd's Avenue
London

Reporting and compliance software solutions



Workiva Inc. (NYSE:WK), provider of the world's leading connected reporting and compliance platform, is used by thousands of enterprises across 180 countries, including 75 percent of Fortune 500® companies, and by government

agencies. Our customers have linked over five billion data elements to trust their data, reduce risk and save time.

 Tim Le Mare

 +44 (0) 203 868 0550

 info@workiva.com

 www.workiva.com/uk

 14 Gray's Inn Road
London
WC1X 8HN
United Kingdom

Risk management software



Since 2014, Origami Risk is the only company that has been consistently recognised for delivering client success, innovation, and stability, while bringing new ideas and advanced features to the RMIS market. Origami Risk's innovative software is designed with the latest technology and a focus on performance and ease-of-use, providing integrated solutions to the entire insurance value chain, serving Risk Managers, Brokers, TPAs and Carriers.

It features powerful workflow, advanced reporting and analysis tools, and intuitive features to improve productivity and better manage total cost of risk—saving our clients time and money and enabling them to be more successful. Learn more at www.origamirisk.com

 Neil Scotcher
 +44 (0) 16179 17740
 nscotcher@origamirisk.com
 www.origamirisk.com
 30 Moorgate
 London
 EC2R 6PJ

Risk management software



In today's rapidly evolving world, business models and organisations are facing increased change and unprecedented levels of scrutiny. With change comes complexity, challenging risk managers to redefine the way they lead an organisation's approach to and

implementation of risk management. Protecht helps organisations through deep understanding, monitoring and management of risk. We provide the complete risk solution—comprised of world-class enterprise risk management, compliance, training and advisory services—to government organisations, key regulators and businesses of all sizes across the world. With 20+ years at the forefront of risk and compliance solutions, millions of incidents managed across thousands of individual risks, and over 25 thousand people attending our training courses to date, we're one of the most respected and influential voices in risk.

 Keith Davies
 +44 (0) 7828 163 802
 keith.davies@protechtgroup.com
 www.protechtgroup.com
 131 Finsbury Pavement
 London
 EC2A 1NT
 United Kingdom

Risk management training



As the world's leading enterprise risk management institute, we know what great risk management looks like, and what risk management professionals need to know, do and deliver to succeed. What's more, we understand how training works and we are experts in designing and delivering courses that provide the tools and motivation to make change happen. Our short courses

and tailored in-house learning and development solutions support hundreds of organisations every year, both in the UK and internationally. Some courses, like the Fundamentals of Risk Management, cover the broad range of ERM skills, whilst others take an in-depth look at specific topics, e.g. Risk Analysis, Risk Appetite and Tolerance, Managing Risk Culture, and Identifying Key Risk Indicators. Members can also benefit from a new suite of e-learning courses, which are now available on our website.

 Sanjay Himatsingani
 +44 (0) 20 7709 4114
 sanjay.himatsingani@theirm.org
 www.theirm.org/training
 IRM Training
 Sackville House,
 143-149 Fenchurch Street,
 London, EC3M 6BN

Playtime

With office life potentially opening up in the near future, it may be time to reintroduce playtime at work

Games are as old as humanity. Among the detritus left behind by ancient civilizations, archaeologists often find traces of play. As well as hockey and handball, for instance, the ancient Egyptians engaged in boardgames and variations on the game of hopscotch.

Some of those ancient activities are still with us. Children use ropes to play skipping games – sometimes accompanied by rhyming songs. Marbles, cat's cradle and conkers make periodic comebacks. And most children love to escape from the confines of the classroom to play tag or kick a ball around.

But the serious study of games did not begin until the end of the 19th century. When the Leiden-based scholar Johan Huizinga published *Homo Ludens*, a study of the play element in culture in 1930, it was controversial and ultimately ignored because it seemed too frivolous a subject to be useful.

In the Sixties, the eminent American professor of comparative literature Rosalie Colie picked up his work and realised that Huizinga's broader point was that in organisations people tended to create rules-based systems in which to work. That is useful, but it can stifle creativity. Play is a potential antidote because it creates spaces where it is okay to break the rules, which can often



Image credit: Unsplash

lead to new ways of doing things.

But the problem with introducing play in the workplace is that it is a voluntary activity. Enforced play is a contradiction in terms. In addition, it should have no real purpose. That is because in play people enter into a kind of fantasy world that has its own set of rules, but in which the consequences have no real impact on ordinary life. Huizinga compares amateur and professional sports people in this regard – a friendly kick-around at five-a-side football is more playful than a professional FA Cup championship final, for example.

That has not prevented Silicon Valley companies introducing pool and ping-pong tables into their campus-style workplaces. Even in such highly-charged cultures of overwork, play seems to have found a place.

In fact, recent studies have

“ Play creates spaces where it is okay to break the rules, which can often lead to new ways of doing things

shown the paranoia of parents over the damaging effects of gaming culture on children to be often unfounded. Professor Andrew Przybylski (<https://bit.ly/2SBhVlq>), director of research at the Oxford Internet Institute, recently found that children enjoyed feelings of competence and social connection after playing games such as the Nintendo blockbuster Animal Crossing.

Perhaps blended working, where people split their time between office and home, could help. As work and life activities continue to merge, playing games with colleagues could become a useful pastime. Having a Fortnite leader board or an Animal Crossing league table, for instance, could help create a more creative and integrated culture at a business than any amount of enforced team-building away-days could ever achieve. 

IRM's revised International Diploma in Risk Management

Advance your career with the global benchmark qualification in Enterprise Risk Management



Already completed an IRM Certificate? You can take these 4 modules to become a GradIRM

The revised International Diploma in Risk Management is the global benchmark for risk professionals and their employers. Students will benefit from our new online learning platform. Students can submit their assignments when they are ready, meaning no more exam centres!

This Master's level equivalent qualification has been developed by internationally recognised academics and industry practitioners to provide you with the knowledge and skills to manage risk and maximise opportunities in any organisation.

Build on your existing knowledge from the International Certificates and become a recognised expert, applicable for all businesses in any sector, and increase your career prospects and earning potential.

Organisations are increasingly looking for GradIRM for senior hires, **make sure it's you.**

What's new about the International Diploma?

- > Students can enrol at any time
- > Learn from anywhere in the world via the VLE
- > Access the learning platform via PC, tablet or mobile phone
- > Assessed through practical work-based assignments that can be submitted online
- > Quicker (provisional) results on marked assignments
- > Potentially shorter study time more suited to those who are working

What our students say



Charlotte Candy CMIRM, Associate, Risk Management Buildings and Places, AECOM

"The IRM Diploma in Enterprise Risk Management has given me invaluable tools and techniques to tackle difficult and sometimes previously unheard of scenarios. IRM qualifications not only provide confidence for employers and clients that you take best practice seriously, but it also gives you access to a huge range of resources and publications." examination and high standard of pass marks."

Find out more at:

www.theirm.org/diploma-mag

Resilience, risk and recovery



Developing risk professionals

Why risk it? Get qualified

Advance your career with the global benchmark qualification in risk management



International Certificate in Enterprise Risk Management



International Certificate in Financial Services Risk Management

Ensure that your company is armed and resilient in these uncertain times.

There's never been a better time to get qualified in risk management, help organisations with the economic recovery post Covid-19 and increase your earning potential and career prospects. Capitalise on opportunities to save your organisation time and money.

IRM's globally recognised International Certificates in Enterprise Risk Management and Financial Services Risk Management can help you to become an effective risk professional, and become current and competent. Both qualifications take 6-9 months to complete, the certificates are delivered by online supported distanced learning.

Gain a whole new skillset from the comfort of your own home.

What our students say



Audrey Onsomu IRMCert, Audit and Assurance Supervisor, PwC

"My IRM qualification is a treasure. I would encourage anyone already pursuing a risk management career or looking to move into risk management to do the certificate. The qualification and study are well set up to ensure you obtain the knowledge that you will need to succeed. My qualification has helped firm up the experience I have had over the last 6 years."

Find out more at:

www.theirm.org/qualifications

Resilience, risk and recovery

irm

Developing risk professionals